Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/SE05/000141

International filing date: 07 February 2005 (07.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/543,545
Filing date: 12 February 2004 (12.02.2004)

Date of receipt at the International Bureau: 04 April 2005 (04.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PA 1285935

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

February 23, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/543,545***
FILING DATE: ***February 12, 2004***

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

N. WOODSON
Certifying Officer

PTO/SB/16 (10-01)
Approved for use through 10/31/2002. OMB 0651-0037
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Customer Number **21839**

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 C.F.R. § 1.53(c).

Docket Number	003301-117	Type a plus sign (+) inside this box	+

INVENTOR(s)/APPLICANT(s)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
ANDERSSON	Jonas		Höllviken, Sweden

☐ *Additional inventors are being named on the ____separately numbered sheets attached hereto.*

TITLE OF THE INVENTION (500 characters max)

PÖRTABEL DATABÄRARE, EXTERN UPPSTÄLLNING, SYSTEM OCH FÖRFARANDEN FÖR TRADLÖS DATAÖVERFÖRING (PORTABLE DATA CARRIER, EXTERNAL ARRANGEMENT, SYSTEM AND METHODS FOR WIRELESS DATA TRANSMISSION)

CORRESPONDENCE ADDRESS

Burns, Doane, Swecker & Mathis, L.L.P.
Customer Number **21839**
Post Office Box 1404
Alexandria

STATE	Virginia	ZIP CODE	22313-1404	COUNTRY	United States of America

ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification Number of Pages 28
☒ Drawing(s) Number of Sheets 3 (Figs. 1 to 4)
☐ Application Data Sheet. See 37 CFR 1.76
☒ Other (specify) Claims 1 to 48 (6 Pages)
Abstract (1 Page)

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)

☒ Applicant claims small entity status. See 37 C.F.R. § 1.27. ☒ A check or money order is enclosed to cover the Provisional filing fees. ☒ The Director is hereby authorized to charge any deficiency in filing fees or credit any overpayment to Deposit Account No. 02-4800. This paper is submitted in duplicate.	**PROVISIONAL FILING FEE AMOUNT(S)**	☒ **$80.00 (2005)** ☐ **$160.00 (1005)**

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE  DATE February 12, 2004

TYPED or PRINTED NAME Benton S. Duffett, Jr. Registration No. 22,030 *(if appropriate)*

PORTABEL DATABÄRARE, EXTERN UPPSTÄLLNING, SYSTEM OCH FÖRFARANDEN FÖR TRÅDLÖS DATAÖVERFÖRING

Uppfinningens område

Föreliggande uppfinning avser en portabel databärare, vilken omfattar ett bärarminne för lagring av data innefattande ett biometriskt templat och en tillämpningsspecifik funktion samt bärarkommunikationsorgan för att kontaktfritt ta emot och sända ut data. Vidare avses ett förfarande, och ett minnesmedium med instruktioner, för överföring av data med hjälp av en portabel databärare enligt ovan.

Föreliggande uppfinning avser även en extern uppställning innefattande uppställningskommunikationsorgan för att kontaktfritt ta emot och sända ut data samt en sensor för att registrera ett biometriskt prov. Vidare avses ett förfarande, och ett minnesmedium med instruktioner, för överföring av data med hjälp av en extern uppställning enligt ovan.

Föreliggande uppfinning avser dessutom ett system för överföring av data innefattande en portabel databärare och en extern uppställning enligt ovan. Vidare avses ett förfarande för överföring av data innefattande ett förfarande för överföring av data med hjälp av en portabel databärare och ett förfarande och för överföring av data med hjälp av en extern uppställning enligt ovan.

Bakgrundsteknik

Tillgången till information, till en lokal eller liknande behöver i många fall vara begränsad till vissa personer. Sådana fall kan exempelvis vara när elektroniska penningtransaktioner ska ske över Internet, när man på ett sjukhus vill begränsa tillgången till journaler, eller när endast vissa personer på en arbetsplats får ha tillgång till viss information eller vissa lokaler. I dessa sammanhang används ofta portabla databärare, t ex

intelligenta kort eller smartcards. Ett smartcard kan beskrivas som ett kort i kontokortsstorlek som har en inbyggd processor eller ett signalbehandlingsorgan, ett minne och ett kommunikationsgränssnitt.

På alla smartcards som används i ovanstående sammanhang finns känslig information lagrad. Denna känsliga information innefattar åtminstone ett så kallat templat vilket kan beskrivas som en i förväg lagrad referensinformation avseende kortanvändaren. Det är med hjälp av detta templat kortanvändarens rätt att använda kortet verifieras vid varje användningsförsök. Beroende på i vilka sammanhang ett smartcard är avsett att användas kan även annan känslig information vara lagrad i kortminnet.

Templatet ovan kan exempelvis svara mot en så kallad pin-kod (PIN = "Personal Identification Number"). När kortinnehavaren vill verifiera sin rätt att använda kortet, placerar han/hon det i en terminal och matar in en pin-kod. Kortinnehavarens kortanvändarrätt verifieras om den inmatade pin-koden överensstämmer med det i minnet lagrade templatet. Templatet ovan kan enligt ett annat exempel vara biometriskt, d v s svara mot kroppsrelaterad, individspecifik information, såsom mönstret på en användares fingrar, handflata, iris, eller användarens röst. Ett förfarande där en kortinnehavare eller kortanvändare identifierar sig med biometrisk information enligt den kända tekniken går typiskt till på följande sätt:

Användaren placerar sitt smartcard i en terminal och ett finger på en sensor som genererar en digital bild, d v s en digital representation, av detta. Den digitala bilden av fingret går vidare till en extern processor, exempelvis en persondator, där den förbehandlas. Vid förbehandlingen minskas informationsmängden i bilden så att exempelvis en binäriserad bild eller delar av en binäriserad bild skapas. En motsvarande förbehandlad bild finns lagrad på kortet som ett templat. Den externa processorn hämtar templatet från kortet och jämför detta med den

förbehandlade bilden av fingret. Kortinnehavarens kortanvändarrätt verifieras om bilden överensstämmer med templatet.

Vid användning av ovan beskrivna portabla databärare måste de av en användare anordnas i fysisk kontakt med en terminal för att kunna kommunicera med densamma. Detta innebär att användaren av en sådan portabel databärare under normala omständigheter således alltid är medveten om när hans/hennes databärare kommunicerar med terminalen. Den för kommunikationen erfordrade fysiska kontakten mellan terminal och databärare är emellertid ibland en källa till problem, bland annat på grund av risken för glapp i kontakten, korrosion på kontaktytorna, osv. För att lösa dessa problem är det känt att använda trådlös kommunikation mellan en portabel databärare och en terminal.

US-patent 6 111 506 beskriver exempelvis ett system där en kortliknande databärare i form av ett personligt identifieringsdokument kommunicerar trådlöst med en terminal. När identifieringsdokumentet tar emot en signal från terminalen kontrollerar det om terminalen har rätt att kommunicera med identifieringsdokumentet. Om så är fallet, tillåts terminalen läsa data från identifieringsdokumentet. De data som läses kan vara biometriska data som t ex representerar ett fingeravtryck för innehavaren av identifieringsdokumentet. Vid en biometrisk identifieringskontroll ombeds personen som uppvisar identifieringsdokumentet att interagera med en till terminalen ansluten anordning för registrering av biometriska data. I en till terminalen ansluten dator jämförs därefter nämnda från identifieringsdokumentet lästa biometriska data med nämnda registrerade biometriska data. Om det föreligger en överensstämmelse mellan dessa är det verifierat att den som uppvisar identifieringsdokumentet är den rätta innehavaren av detsamma. I fallet med detta system aktiveras alltså identifieringsdokumentet för läsning av terminalen så snart det har konstaterats att ter-

minalen har rätt att kommunicera med identifieringsdokumentet. Detta innebär således att identifieringsdokumentets data är öppna för avläsning oberoende av om det är den rättmätiga innehavaren av identifieringsdokumentet som uppvisar detsamma eller någon som t ex har stulit identifieringsdokumentet. Konstruktionen av systemet enligt ovan medför vidare problemet att kommunikation med databäraren utan dess bärares vetskap möjliggörs. En terminal i orätta händer kan exempelvis i hemlighet anordnas i närheten av t ex en väska eller en ficka innehållande databäraren och därifrån läsa data lagrade i, eller på annat sätt interagera med, databäraren. Detta innebär ett stort problem i många situationer. Ett exempel är om identifieringsdokumentet är ett pass och innehavaren av passet av någon anledning inte vill avslöja sin nationalitet eller annan information som är lagrad i passet. Passets innehavare kanske till och med vill hemlighålla blotta innehavet av passet. Det sistnämnda resonemanget kan även tillämpas i samband med identifieringsdokument i form av medlemskort för olika organisationer, varvid medlemskapet önskas hemlighållas. Slutligen, om ett system motsvarande det ovanstående skulle tillämpas i samband med en databärare i form av ett bankkort skulle detta kunna innebära att någon med en portabel terminal relativt enkelt skulle kunna stjäla pengar direkt från bankkortskontot.

US-patent 5 484 997 beskriver ett system i vilket en kortliknande databärare i form av ett identitetskort kommunicerar trådlöst med en terminal. Identitetskortet aktiveras att automatiskt sända ut i detsamma lagrade data när fotoceller på identitetskortet bestrålas. Om identitetskortet inte skyddas i t ex en plånbok eller börs när det inte är avsett att användas, kan det alltså på ett oönskat sätt sända ut data till terminaler i närheten. Vidare gäller att det måste finnas en tillräcklig bestrålning vid användning av databäraren för att den ska kunna fungera. Således finns en risk för att databäraren

inte kan användas om den inte är anordnad på ett visst sätt i förhållande till strålningskällan eller om användaren av misstag lägger sina fingrar över fotocellerna. Slutligen är det svårt att tillverka en hållbar och praktiskt utformad databärare av ovan nämnda slag.

Sammanfattning av uppfinningen

Ändamålet med föreliggande uppfinning är att helt eller delvis eliminera de problem som är associerade med känd teknik.

Detta ändamål uppnås med en portabel databärare, ett förfarande, och ett minnesmedium med instruktioner, för överföring av data med hjälp av en portabel databärare, en extern uppställning, ett förfarande, och ett minnesmedium med instruktioner, för överföring av data med hjälp av en extern uppställning samt ett system och ett förfarande för överföring av data enligt de bifogade oberoende patentkraven. Utföringsformer av uppfinningen anges i de efterföljande beroende patentkraven.

En grundtanke med föreliggande uppfinning är att förhindra att känsliga data lagrade i en portabel databärare läses utan dess bärares vetskap och medgivande. En annan grundtanke med föreliggande uppfinning är att förhindra att känsliga data lagrade i en portabel databärare läses utan dess rättmätige innehavares vetskap och medgivande. Sammanfattningsvis är syftet med föreliggande uppfinning bland annat att förhindra att känsliga data lagrade i en portabel databärare läses utan att det har kontrollerats att den som bär den portabla databäraren är den rättmätige innehavaren av densamma och att denne innehavare har gett sitt samtycke till läsningen.

Uppfinningen avser enligt en första aspekt närmare bestämt en portabel databärare vilken omfattar ett bärarminne för lagring av data innefattande ett biometriskt templat och en tillämpningsspecifik funktion samt bärarkommunikationsorgan för att kontaktfritt ta emot och sända ut data. Den portabla databäraren utmärkes av att den vidare omfattar bärarbehandlingsorgan för att jämföra det

biometriska templatet med ett från en extern uppställning mottaget biometriskt prov och är anordnad att utföra den tillämpningsspecifika funktionen och sända ett resultat av densamma till den externa uppställningen endast om det biometriska provet matchar det biometriska templatet.

Med databärare avses en rad olika enheter, både passiva och aktiva sådana, som exempelvis smartcards, elektroniska pass, elektroniska visum och biljetter, så kallade "RF-tags", mobiltelefoner, så kallade "PDAs" ("Personal Digital Assistants") etc. Med begreppet passiv databärare avses en databärare som inte har någon egen energiförsörjning och således är beroende av en yttre energikälla för att kunna arbeta. Med begreppet aktiv databärare avses motsatsen, d v s en databärare som har egen energiförsörjning. Valet mellan en passiv och aktiv databärare görs efter den tillämpning i vilken databäraren är avsedd att användas. Med begreppen biometriskt templat respektive biometriskt prov avses individspecifika data, d v s data som är unika för varje individ. Några exempel på sådana data kan vara mönstret på individens fingrar, handflata, iris, eller individens ansikte, röst eller DNA. Templatet avser referensdata som är lagrade på databäraren och normalt inte ändras efter den ursprungliga lagringen. Provet avser data som måste presenteras av en individ varje gång denne vill använda den portabla databäraren.

Att den portabla databäraren innefattar bärarkommunikationsorgan för kontaktfri, d v s beröringsfri, överföring av data, medför att de med känd teknik förknippade kontaktproblemen elimineras, exempelvis problem som att kontaktytorna förstörs eller slits ut. Den kontaktfria överföringen innebär vidare att den portabla databäraren inte måste anordnas i direkt anslutning till den externa uppställningen för att kommunikation skall kunna ske dem emellan. Teoretiskt sett behöver en användare inte ens ta fram sin databärare ur exempelvis fickan eller väskan vid kommunikationen med den externa uppställningen. Detta kan

vara praktiskt i fallet att användaren har andra ting i händerna, såsom t ex flygbiljetter eller resväskor. Det är också praktiskt ur den synpunkten att användaren på detta sätt inte behöver leta runt i exempelvis sin väska efter databäraren och heller inte riskerar att tappa bort databäraren.

Det faktum att den portabla databäraren innefattar bärarbehandlingsorgan för att jämföra det biometriska templatet med det biometriska prov som tas emot från den externa uppställningen medför att det biometriska templatet inte behöver lämna databäraren vid denna biometriska jämförelse, vilket är positivt ur säkerhetssynpunkt.

Särdraget att den portabla databäraren är anordnad att utföra den tillämpningsspecifika funktionen och sända ett resultat av densamma till den externa uppställningen endast under förutsättning att det biometriska provet matchar det biometriska templatet, innebär att eventuellt känslig information skyddas från omvärlden tills det har verifierats att den som bär den portabla databäraren verkligen är den rättmätiga innehavaren av densamma.

Med matchning menas i detta sammanhang att det biometriska provet överensstämmer med det biometriska templatet i tillräckligt hög grad för att den som bär den portabla databäraren ska anses vara densamma som databärarens rättmätiga innehavare.

Med begreppet tillämpningsspecifik funktion avses en uppsättning instruktioner enligt vilka databäraren är anordnad att arbeta under vissa förutsättningar. Sammansättningen av dessa instruktioner är beroende av i vilken tillämpning den portabla databäraren är avsedd att användas.

Den tillämpningsspecifika funktionen i databäraren kan omfatta instruktionen att från bärarminnet hämta däri lagrad tillämpningsspecifik information, varvid resultatet som sänds till den externa uppställningen innefattar den tillämpningsspecifika informationen. Sammansättningen av den tillämpningsspecifika informationen är beroende av

i vilken tillämpning den portabla databäraren är avsedd att användas. Den kan exempelvis vara information som finns lagrad på själva databäraren i form av datafiler, en "nyckel" som gör att databäraren kan utnyttjas för att exempelvis öppna en dörr till ett rum och ge användaren tillgång till information av en annan typ än vad som kan lagras på själva databäraren, eller olika typer av så kallade digitala certifikat. I fallet att databäraren exempelvis är avsedd att användas som ett elektroniskt pass, kan den tillämpningsspecifika informationen innehålla sådan information som innefattas i traditionella pass, d v s exempelvis information som identifierar innehavaren av det elektroniska passet.

Den tillämpningsspecifika funktionen i databäraren kan dessutom/alternativt omfatta instruktionen att exekvera programkod som finns lagrad i bärarminnet. Exekvering av denna programkod gör det möjligt för databäraren att tillhandahålla olika slags funktionalitet, såsom kryptering, signering, verifiering, evaluering etc. I fallet att databäraren är en mobiltelefon med bankkortsfunktionalitet, kan exekvering av programkoden medföra en signering av en penningtransaktion, vilken signering innefattas i resultatet som sänds till den externa uppställningen.

Den portabla databäraren kan vara anordnad att utföra den tillämpningsspecifika funktionen samt sända nämnda resultat av densamma till den externa uppställningen som svar på en från den externa uppställningen mottagen förfrågan. En sådan förfrågan kan innebära att den externa uppställningen ber den portabla databäraren att sända över information och/eller utföra nämnda funktion baserat på vissa parametrar.

Det biometriska templatet kan svara mot en digital bild, d v s en registrering i digital form, innefattande individspecifik information enligt ovan. Fördelen med att använda digitala representationer är att de går lätt och

snabbt att registrera och att de är enkla att behandla på olika sätt.

Det biometriska templatet kan definiera åtminstone en del av ett fingeravtryck, vilken del företrädesvis har ett speciellt intressant informationsinnehåll svarande mot t ex intressanta skärningspunkter mellan linjer i fingeravtrycket. Fördelen med användning av fingeravtryck för biometrisk identifiering är bland annat att ett fingeravtryck från en och samma individ under normala omständigheter är oföränderligt. Fingeravtryck är dessutom enkla att registrera med hjälp av konventionella sensorer.

Det biometriska templatet kan svara mot särdragsreferensdata som exempelvis beskriver de mest utmärkande särdragen i ett fingeravtryck från innehavaren av den portabla databäraren. Genom denna utföringsform kan mindre information jämföras för att konstatera om biometrisk matchning föreligger eller inte än om det biometriska templatet svarar mot hela fingeravtrycket.

Det biometrisk templatet kan vidare svara mot en kombination av ovanstående olika alternativ, exempelvis en kombination av en bild av åtminstone en del av ett fingeravtryck och särdragsreferensdata för fingeravtrycket.

Den portabla databäraren kan vara anordnad att i bärarminnet lagra ett tröskelvärde som definierar i vilken grad det biometriska provet ska överensstämma med det biometriska templatet för att en matchning ska anses föreligga. I detta fall är databäraren anordnad att med hjälp av nämnda bärarbehandlingsorgan bestämma ett värde på överensstämmelsen mellan det biometriska provet och det biometriska templatet och sedan jämföra detta värde med tröskelvärdet. Om värdet på överensstämmelsen överstiger tröskelvärdet anses matchning enligt ovanstående definition föreligga, och vice versa. Tröskelvärdet kan väljas och anpassas efter den tillämpning i vilken den portabla databäraren är avsedd att användas. Om databär-

aren exempelvis är ett elektroniskt pass kan ett högre tröskelvärde väljas än om databäraren är ett enklare "nyckelkort", vilket t ex kan användas för att generera ett medgivande eller nekande till fysisk access till en lokal.

Den portabla databäraren kan vara ett elektroniskt pass avsett att ersätta de vanliga traditionella passen. Ett sådant elektroniskt pass kan enligt en utföringsform utgöras av ett vanligt pass som är försett med ett datorchip med förmåga att lagra, överföra och behandla data. En sådan utföringsform skulle innebära att de vanliga passen inte måste kasseras utan kan anpassas till den nya tekniken genom att de kompletteras med ett chip enligt ovan. Ett elektroniskt pass enligt uppfinningen kan naturligtvis utformas på ett flertal andra sätt utan att avvika från uppfinningens omfattning såsom den definieras av de bifogade kraven.

Med ett elektroniskt pass enligt föreliggande uppfinning blir en passkontroll både enklare och säkrare. Istället för att en passkontrollant manuellt måste utföra passkontrollen genom att jämföra den person som visar upp passet med den person som visas på bilden i passet, vilket kan vara en svår, tidskrävande och felbenägen uppgift, behöver endast en registrering av ett biometriskt prov göras som resulterar i ett besked om en person verkligen är den han/hon utger sig för att vara.

Såsom angetts ovan behöver det biometriska templatet inte lämna den portabla databäraren för att jämförelse med ett biometriskt prov ska kunna utföras. Den portabla databäraren kan vara anordnad att helt och hållet förhindra yttre åtkomst till det biometriska templatet.

Den portabla databäraren kan vara anordnad att kommunicera med den externa uppställningen endast under en förutbestämd tid efter att matchning har ansetts föreligga. Efter att den förutbestämda tiden har förflutit är databäraren då anordnad att avbryta kommunikationen med den externa uppställningen. Denna förutbestämda tid är

företrädesvis precis så lång att resultatet av utförandet av den tillämpningsspecifika funktionen hinner överföras. Ett sådant automatiskt brott av kommunikationslänken mellan den externa uppställningen och databäraren ökar säkerheten mot otillåten läsning av känslig information från databäraren.

En portabel databärare enligt uppfinningen kan vara anordnad att sända ut en närvarosignal som svar på en från den externa uppställningen mottagen söksignal för att bekräfta sin närvaro inom en kommunikationsräckvidd för den externa uppställningen. Fördelarna med en sådan utföringsform diskuteras nedan i samband med den externa uppställningen enligt uppfinningen.

En portabel databärare enligt uppfinningen kan istället vara anordnad att förhindra all utsändning av data från densamma tills matchning anses föreligga. Fördelen med en sådan utföringsform är att en person inte avslöjar sitt innehav av en portabel databärare enligt uppfinningen mot sin vilja. Personen måste aktivt ge sitt medgivande till att avslöja sitt databärarinnehav genom att lämna ett biometriskt prov. Det biometriska provet sänds sedan ut till samtliga portabla databärare enligt uppfinningen som befinner sig inom en kommunikationsräckvidd för den externa uppställningen där provet lämnades. Bara en portabel databärare som innehåller ett matchande biometriskt templat kan därefter avslöja sin existens.

Föreliggande uppfinning avser enligt en andra aspekt ett förfarande för överföring av data med hjälp av en portabel databärare vilken omfattar ett bärarminne för lagring av data innefattande ett biometriskt templat och en tillämpningsspecifik funktion samt bärarkommunikationsorgan för att kontaktfritt ta emot och sända ut data. Förfarandet utmärkes av att det vidare innefattar att ta emot ett biometriskt prov från en extern uppställning, att med hjälp av bärarbehandlingsorgan i databäraren jämföra det biometriska provet med det biometriska templatet, och att utföra den tillämpningsspecifika funk-

tionen och sända ett resultat av densamma till den externa uppställningen endast om det biometriska provet matchar det biometriska templatet.

Föreliggande uppfinning avser enligt en tredje aspekt ett minnesmedium innefattande ett datorprogram med instruktioner vilka är anordnade att vid exekvering utföra förfarandet ovan.

Särdragen som diskuterades ovan i samband med den portabla databäraren är naturligtvis överförbara till förfarandet och minnesmediet enligt den andra respektive tredje aspekten av uppfinningen. Vidare gäller att ovanstående särdrag naturligtvis är kombinerbara i samma utföringsform.

Föreliggande uppfinning avser enligt en fjärde aspekt en extern uppställning innefattande uppställningskommunikationsorgan för att kontaktfritt ta emot och sända ut data samt en sensor för att registrera ett biometriskt prov. Den externa uppställningen utmärkes av att den är anordnad att sända det biometriska provet till en portabel databärare och ta emot, endast om det biometriska provet matchar ett i den portabla databäraren lagrat biometriskt templat, ett resultat av en i den portabla databäraren utförd tillämpningsspecifik funktion från databäraren.

Den externa uppställningen kan vara anordnad att som nämnda resultat ta emot i databäraren lagrad tillämpningsspecifik information.

Den externa uppställningen kan vara anordnad att ta emot nämnda resultat som svar på en till den portabla databäraren sänd förfrågan.

I fallet att det biometriska templatet i bärarminnet svarar mot en digital bild innefattande individspecifik information bör detta gälla även det biometriska provet.

I fallet att det biometriska templatet i bärarminnet definierar åtminstone en del av ett fingeravtryck bör detta gälla även det biometriska provet.

I fallet att det biometriska templatet svarar mot särdragsreferensdata bör det gälla att det biometriska provet svarar mot särdragsdata.

I fallet att det biometrisk templatet svarar mot en kombination, bör det gälla att det biometriska provet svarar mot en motsvarande kombination av ovanstående olika alternativ.

Den externa uppställningen kan vara anordnad att sända ut en söksignal och som svar på söksignalen ta emot en närvarosignal från den portabla databäraren för att detektera dess närvaro inom en kommunikationsräckvidd för den externa uppställningen. I en sådan utföringsform kan den externa uppställningen aktiveras för registrering genom mottagandet av närvarosignalen, vilket ger fördelen att ett biometriskt prov varken kan registreras eller sändas ut i onödan, d v s om ingen portabel databärare som kan ta emot det biometriska provet finns inom kommunikationsräckvidden för den externa uppställningen, vilket innebär en energibesparing. I en alternativ utföringsform är den externa uppställningen alltid aktiv.

Den externa uppställningen kan vara anordnad att sända ut det biometriska provet enligt ett förutbestämt schema tills matchning anses föreligga. I en sådan utföringsform kan ett biometriskt prov, så snart det har registrerats, sändas till samtliga portabla databärare enligt uppfinningen som befinner sig inom en kommunikationsräckvidd för den externa uppställningen. Den externa uppställningen kan i detta fall vara helt omedveten om existensen av eventuella portabla databärare tills biometrisk jämförelse har utförts i en portabel databärare som innehåller ett matchande biometriskt templat. Ovanstående utsändningsschema för det biometriska provet kan anpassas efter omständigheterna, d v s den tillämpning i vilken den externa uppställningen är avsedd att användas. Utsändningsschemat kan exempelvis innebära att det biometriska provet utsänds med bestämda intervaller.

Att den externa uppställningen är anordnad enligt ovanstående olika utföringsformer medför att den kan fungera tillfredsställande med de olika utföringsformerna av den portabla databäraren enligt den första aspekten av uppfinningen för att uppnå de ovan beskrivna fördelarna.

Föreliggande uppfinning avser enligt en femte aspekt ett förfarande för överföring av data med hjälp av en extern uppställning, vilken innefattar uppställningskommunikationsorgan för att kontaktfritt ta emot och sända ut data samt en sensor, innefattande att med hjälp av sensorn registrera ett biometriskt prov. Förfarandet utmärkes av att det vidare innefattar att sända det biometriska provet till en portabel databärare, och att ta emot, endast om det biometriska provet matchar ett i den portabla databäraren lagrat biometriskt templat, ett resultat av en i den portabla databäraren utförd tillämpningsspecifik funktion från databäraren.

Föreliggande uppfinning avser enligt en sjätte aspekt ett minnesmedium innefattande ett datorprogram med instruktioner vilka är anordnade att vid exekvering utföra förfarandet enligt den femte aspekten av uppfinningen.

Särdragen som diskuterades ovan i samband med den externa uppställningen är naturligtvis överförbara till förfarandet och minnesmediet enligt den femte respektive sjätte aspekten av uppfinningen. Vidare gäller att ovanstående särdrag naturligtvis är kombinerbara i samma utföringsform.

Föreliggande uppfinning avser enligt en sjunde aspekt ett system för överföring av data innefattande en portabel databärare enligt den första aspekten av uppfinningen och en extern uppställning enligt den fjärde aspekten av uppfinningen.

Föreliggande uppfinning avser enligt en åttonde aspekt ett förfarande för överföring av data innefattande ett förfarande enligt den andra aspekten av uppfinningen

och ett förfarande enligt den femte aspekten av uppfinningen.

Förfaranden enligt uppfinningen kan såsom anges ovan implementeras som datorprogram som lagras i ett minne och exekveras i nämnda behandlingsorgan eller i en extern anordning. Alternativt kan förfarandena helt eller delvis implementeras i form av produktanpassade kretsar, såsom ASICs, eller i form av digitala eller analoga kretsar eller i någon lämplig kombination av dessa.

Särdragen som diskuterades ovan i samband med den portabla databäraren och den externa uppställningen samt de motsvarande förfarandena för dataöverföring med hjälp av dessa, är naturligtvis överförbara till systemet respektive förfarandet enligt den sjunde respektive åttonde aspekten av uppfinningen.

De definitioner av begrepp som har getts ovan i samband med beskrivningen av den första till tredje aspekten av föreliggande uppfinning gäller även den fjärde till åttonde aspekten av föreliggande uppfinning.

Kort beskrivning av ritningarna

Uppfinningen kommer att beskrivas närmare nedan med hänvisning till de bifogade schematiska ritningarna, vilka åskådliggör exempel på utföringsformer av uppfinningen.

Fig 1 är en ritning som visar en portabel databärare enligt en utföringsform av uppfinningen.

Fig 2 är en ritning som visar en extern uppställning enligt en utföringsform av uppfinningen.

Fig 3 är ett flödesschema som åskådliggör ett förfarande för överföring av data med hjälp av en portabel databärare enligt en utföringsform av uppfinningen.

Fig 4 är ett flödesschema som åskådliggör ett förfarande för överföring av data med hjälp av en extern uppställning enligt en utföringsform av uppfinningen.

Beskrivning av föredragna utföringsformer

I fig 1 visas schematiskt en portabel databärare 10 i form av ett elektroniskt pass enligt uppfinningen. I

fig 2 visas schematiskt en extern uppställning 20 enligt uppfinningen. Den portabla databäraren 10 och den externa uppställningen 20 ingår i ett system i vilket de är anordnade att kontaktlöst och beröringsfritt kommunicera med varandra enligt kända protokoll för RF-kommunikation, t ex ISO 14443. För detta ändamål innefattar de bärarkommunikationsorgan 11 respektive uppställningskommunikationsorgan 21.

Den portabla databäraren 10, vilken har en funktion som delvis påminner om funktionen för ett standardmässigt smartcard, exempelvis ett Java- eller MULTOS-kort, omfattar ett bärarminne 12 för lagring av data innefattande ett biometriskt templat 13, tillämpningsspecifik information 14 och en tillämpningsspecifik funktion 15. Registrering och lagring av det biometriska templatet 13 kan göras på något känt sätt, exempelvis på något av de sätt som beskrivs i sökandens patentpublikationer WO01/11577, WO01/84494, WO01/06445 och WO03/003286, vilka härmed införlivas häri genom denna hänvisning. I föreliggande utföringsform svarar det biometriska templatet 13 mot data för ett fingeravtryck från det elektroniska passets rättmätige innehavare. Såsom namnet antyder beror sammansättningen av den tillämpningsspecifika informationen 14 på det sammanhang i vilket den portabla databäraren är avsedd att användas. I föreliggande utföringsform, där den portabla databäraren är ett elektroniskt pass, innefattar den tillämpningsspecifika informationen data som beskriver innehavaren av den portabla databäraren, d v s sådana data som innefattas i traditionella pass, t ex data som anger innehavarens ålder och nationalitet samt uppgifter om vem som har utfärdat passet. Den tillämpningsspecifika funktionen 15 innefattar en uppsättning instruktioner enligt vilka den portabla databäraren är anordnad att arbeta under vissa förutsättningar. Såsom namnet antyder beror sammansättningen av dessa instruktioner på det sammanhang i vilket den portabla databäraren är avsedd att användas. I denna utföringsform om-

fattar den tillämpningsspecifika funktionen instruktionen att hämta den tillämpningsspecifika informationen 14 från bärarminnet och sända den till den externa uppställningen. Detta skall göras under förutsättning att biometrisk matchning har konstaterats, handskakning har utförts med den externa uppställningen 20 och en förfrågan om informationsöverföring har mottagits från den externa uppställningen, vilket kommer att förklaras mer detaljerat nedan i samband med beskrivningen av fig 3 och 4.

Den portabla databäraren 10 har slutligen bärarbehandlingsorgan 16 i form av en processor som använder programvara, vilken är lagrad i bärarminnet 12, för att bearbeta data i den portabla databäraren. Processorn utför exempelvis ovannämnda biometriska matchning, handskakning och tillämpningsspecifika funktion.

Den externa uppställningen 20, vilken i föreliggande utföringsform är en extern uppställning konstruerad för kommunikation med ett elektroniskt pass, d v s för elektronisk passkontroll, omfattar ett uppställningsminne 22 för lagring av data innefattande ett biometriskt prov 23. Registrering och lagring av det biometriska provet kan göras på något känt sätt, exempelvis på något av de sätt som beskrivs i sökandens ovan angivna, häri införlivade, patentpublikationer. Eftersom det biometriska templatet 13 i föreliggande utföringsform svarar mot data för ett fingeravtryck från det elektroniska passets 10 rättmätige innehavare, svarar det biometriska provet 23 mot data för ett fingeravtryck från den person som bär det elektroniska passet, vilken person inte nödvändigtvis är den rättmätige innehavaren.

Den externa uppställningen 20 innefattar vidare en sensor 25 som är anordnad att registrera det biometriska provet 23 innan detta lagras i uppställningsminnet 22. I föreliggande utföringsform är sensorn 25 en kapacitiv sensor som registrerar fingeravtryck. Emellertid kan även andra kända typer av sensorer användas i samband med föreliggande uppfinning, såsom exempelvis värmesensorer

eller optiska sensorer. Slutligen har den externa uppställningen 20 uppställningsbehandlingsorgan 26 i form av en processor som använder programvara, vilken är lagrad i uppställningsminnet 22, för att bearbeta data i den externa uppställningen. Processorn utför exempelvis handskakning med den portabla databäraren 10, vilket kommer att diskuteras i närmare detalj nedan i samband med beskrivningen av fig 3 och 4. Kommunikationen mellan de olika ingående enheterna i den portabla databäraren, respektive i den externa uppställningen, sker via en databuss (visas ej).

Fig 3 och 4 åskådliggör tillsammans en metod för överföring av data i systemet bestående av den portabla databäraren 10 enligt fig 1 och den externa uppställningen 20 enligt fig 2. Fig 3 åskådliggör det förfarande (steg B1-B10) som utförs i den portabla databäraren, d v s det elektroniska passet, vid dataöverföringen, medan fig 4 åskådliggör det förfarande (steg U1-U10) som utförs i den externa uppställningen vid dataöverföringen.

I föreliggande utföringsform används metoden för dataöverföring i systemet ovan för att genomföra kontaktlös passkontroll. En person som skall passkontrolleras med hjälp av sitt elektroniska pass 10 närmar sig passkontrollen där en extern uppställning 20 är anordnad. Inledningsvis i metoden sänder den externa uppställningen 20, med hjälp av nämnda uppställningskommunikationsorgan 21, trådlöst ut en söksignal (U1) för att detektera förekomsten av en portabel databärare inom ett avstånd som definierar den externa uppställningens kommunikationsräckvidd. När personen ovan, och därmed hans/hennes elektroniska pass 10, kommer inom kommunikationsräckvidden för den externa uppställningen, kraftsätter denna det elektroniska passet enligt någon känd metod med hjälp av en antenn anordnad i det elektroniska passet (visas inte), varvid passet då aktiveras för mottagning av den söksignal som sänds ut av den externa uppställningen. Efter att det elektroniska passet har kraftsatts, kon-

trollerar det (B1) om en söksignal tas emot. Om en söksignal tas emot från den externa uppställningen, sänder det elektroniska passet 10 med hjälp av nämnda bärarkommunikationsorgan 11 ut en närvarosignal (B2) för att bekräfta sin närvaro inom kommunikationsräckvidden för den externa uppställningen. Om en söksignal inte tas emot upprepas kontrollen (B1). Upprepningen görs så länge det elektroniska passet befinner sig inom den externa uppställningens kommunikationsräckvidd. Så snart det elektroniska passet kommer utanför kommunikationsräckvidden upphör dess kraftsättning varvid det elektroniska passet "dör". Efter att den externa uppställningen har sänt ut en söksignal (U1) kontrollerar den (U2) om en närvarosignal tas emot under en förutbestämd söktid efter utsändningen av söksignalen. Om en närvarosignal inte tas emot under denna förutbestämda söktid, sänder den externa uppställningen ut en ny söksignal. Om däremot en närvarosignal tas emot under den förutbestämda söktiden, betyder det att åtminstone en portabel databärare, som eventuellt är ett elektroniskt pass, finns i närheten.

I nästa steg, under förutsättning att närvaron av en portabel databärare har konstaterats, aktiveras den externa uppställningen 20 för registrering, varvid personen ovan kan placera sitt finger på sensorn 25 för registrering av ett biometriskt prov på något av ovan angivna kända sätt (U3). Efter att den externa uppställningen har registrerat det biometriska provet, sänds detta trådlöst med hjälp av nämnda uppställningskommunikationsorgan 21 till det elektroniska passet (U4). Samtidigt undersöker det elektroniska passet om ett biometriskt prov tas emot (B3) under en förutbestämd mottagningstid efter utsändningen av närvarosignalen. Detta sker naturligtvis under förutsättning att det elektroniska passet fortfarande befinner sig inom den externa uppställningens kommunikationsräckvidd. Om inget biometriskt prov tas emot under den förutbestämda mottagningstiden avbryts kommunikationen med den externa uppställningen (B7). I annat fall jäm-

för det elektroniska passet 10, med hjälp av nämnda bärarbehandlingsorgan 16, det mottagna biometriska provet med det lagrade biometriska templatet (B4) för att konstatera om det föreligger en matchning mellan dessa, d v s för att kontrollera om det biometriska provet och det biometriska templatet härstammar från samma person. Vid jämförelsen beräknas ett värde på korrelationen mellan det biometriska provet och det biometriska templatet, och detta korrelationsvärde vägs därefter mot ett förutbestämt tröskelvärde som finns lagrat i bärarminnet 12. Om korrelationsvärdet överstiger tröskelvärdet anses matchning föreligga. I annat fall anses matchning inte föreligga.

Om matchningskontrollen (B5) ger ett positivt utslag, sänds ett meddelande om matchning från det elektroniska passet till den externa uppställningen. Om matchningskontrollen istället ger ett negativt utslag, avbryts kommunikationen med den externa uppställningen (B7). Under en förutbestämd matchningstid efter överföringen av det biometriska provet kontrollerar den externa uppställningen om ett meddelande om matchning tas emot (U5). Om ett sådant meddelande om matchning tas emot utförs någon känd handskakningsprocedur (B6, U6) mellan det elektroniska passet 10 och den externa uppställningen 20. Om ett meddelande om matchning däremot inte tas emot under den förutbestämda matchningstiden avbryts kommunikationen mellan det elektroniska passet och den externa uppställningen (U7).

I föreliggande utföringsform utförs trevägshandskakning enligt någon känd metod, t ex "Mutual Three Pass Authentication" som beskrivs i "Philips Mifare", referens ISO/IEC 9798-2. I föreliggande utföringsform innebär mottagandet av ett meddelande om matchning, d v s ett positivt utslag i kontrollen (U5) på uppställningssidan, att det elektroniska passet, inom den förutbestämda matchningstiden efter utsändningen av det biometriska provet, initierar handskakningsproceduren ovan. Genom att

det elektroniska passet initierar handskakningen, får den externa uppställningen veta att matchning föreligger. I en alternativ utföringsform kan istället den externa uppställningen vara anordnad att initiera handskakningsproceduren. I det fallet innebär meddelandet om matchning inte initierandet av en handskakning utan bara översändandet av en signal som säger att matchning föreligger.

Utförandet av handskakningsproceduren (B6) innebär att det elektroniska passet kontrollerar om den externa uppställningen är av rätt "typ", d v s av den typ som det elektroniska passet är anordnad att kommunicera "fullt ut" med. På samma sätt innebär utförandet av handskakningsproceduren (U6) att den externa uppställningen kontrollerar om den portabla databäraren är av rätt "typ", d v s av den typ som den externa uppställningen är anordnad att kommunicera "fullt ut" med. Rätt typ av extern uppställning för ett elektroniskt pass är en extern uppställning avsedd för passkontroll, och vice versa.

En lyckad utgång av ovanstående handskakningsprocedur (B6, U6) innebär att de båda kontrollerna av om handskakningen är ok (B8, U8) ger positiva utslag. En misslyckad utgång av ovanstående handskakningsprocedur (B6, U6) innebär att åtminstone en av de båda kontrollerna av om handskakningen är ok (B8, U8) ger ett negativt utslag. I föreliggande utföringsform, där det elektroniska passet initierar trevägshandskakningen, måste utslaget av handskakningskontrollen i det elektroniska passet (B8) vara positiv för att handskakningskontrollen i den externa uppställningen (U8) ska ge ett positivt utslag. Ett sådant positivt utslag innebär att det elektroniska passet och den externa uppställningen får kommunicera fullt ut med varandra. Den externa uppställningen sänder då en förfrågan (U9) om översändning av tillämpningsspecifik information till det elektroniska passet. Samtidigt kontrollerar det elektroniska passet om en sådan förfrågan tas emot (B9) från den externa uppställningen inom en förutbestämd förfrågningstid efter utförandet av hand-

skakningsproceduren. Om så inte sker, avbryts kommunikationen med den externa uppställningen (B7). Om däremot nämnda förfrågan tas emot inom förfrågningstiden överförs den efterfrågade tillämpningsspecifika informationen från det elektroniska passet till den externa uppställningen (B10, U10) innan kommunikationen avbryts (B7, U7). I föreliggande utföringsform kan ett negativt utslag av handskakningskontrollen i den externa uppställningen (U8) antingen innebära ett positivt eller ett negativt utslag av handskakningskontrollen i det elektroniska passet (B8). I vilket fall som helst betyder detta att det elektroniska passet och den externa uppställningen inte får kommunicera fullt ut med varandra, varvid kommunikationen dem emellan bryts.

När överföringen av den tillämpningsspecifika informationen från det elektroniska passet till den externa uppställningen är avslutad, kan det vara möjligt för en passkontrollant att titta på den tillämpningsspecifika informationen med hjälp av en visningsenhet, t ex en datorskärm (visas inte). I detta sammanhang kan det även vara möjligt för passkontrollanten att med hjälp av inmatningsorgan (visas inte) registrera nya data i det elektroniska passets minne, såsom t ex data som anger att ett land har besökts av passets innehavare, när innehavaren kom till, och när han/hon lämnade landet, d v s data som i dagens pass registreras genom stämpling i passet.

För att förenkla beskrivningen av utföringsformen ovan har endast en portabel dataanordning diskuterats i anslutning till en extern uppställning. Denna förenklade utföringsform speglar dock sannolikt en realisering av uppfinningen eftersom kommunikationsräckvidden för de externa uppställningar som i dagsläget avses för elektronisk passkontroll är begränsad och ligger inom området 10-15 cm. En sådan relativt liten räckvidd gör att kommunikation mellan en extern uppställning och flera portabla databärare på en och samma gång blir ganska osannolik eftersom det skulle innebära att innehavarna av de por-

tabla databärarna skulle stå och trängas i direkt anslutning till den externa uppställningen. Kommunikationsräckvidden för en extern uppställning enligt ovan skulle kunna förlängas genom att öka sändningseffekten hos kommunikationsorganen. Detta skulle dock medföra att en strålningsnivå från den externa uppställningen skulle kunna öka till ett värde som ligger över gränsvärdet. I vilket fall som helst är en funktion för antikollision implementerad i ovanstående utföringsform så att en extern uppställning kan hålla ordning på vilken portabel databärare den kommunicerar med om flera portabla databärare finns inom den externa uppställningens kommunikationsräckvidd. Vidare gäller att signalerna och informationen som överförs i ovanstående utföringsform är krypterade. Alternativa utföringsformer där kryptering inte används är naturligtvis möjliga.

För tydlighetens skull bör det påpekas att stegen i systemförfarandet för överföring av data mellan en extern uppställning och en portabel databärare bara kan utföras då den portabla databäraren finns inom kommunikationsräckvidden för den externa uppställningen. I utföringsformen ovan, om det elektroniska passet kommer utanför den externa uppställningens kommunikationsräckvidd, måste systemförfarandet utföras på nytt från början om och när det elektroniska passet återigen kommer inom kommunikationsräckvidden. Således kan samtliga steg i systemförfarandet endast utföras om det elektroniska passet finns inom kommunikationsräckvidden under en sammanhängande tid som är tillräckligt lång för att alla stegen i systemförfarandet ska hinna utföras.

Ovanstående metod och konstruktion av den portabla databäraren och den externa uppställningen innebär att det krävs en kontroll som visar att den som använder en portabel databärare verkligen är den rättmätiga innehavaren av densamma innan en extern uppställning överhuvudtaget kan få reda på databärarens typ. En sådan innehavarkontroll kräver i enlighet med vad som beskrivits ovan

användarens medgivande och interaktion, varvid obehörig läsning av data från den portabla databäraren därigenom förhindras. Läsning av personlig och eventuellt känslig information medges vidare inte utan förbehåll även om innehavarkontrollen har positiv utgång. Det krävs dessutom en "handskakningskontroll" för att verifiera att den externa uppställningen och den portabla databäraren är avsedda att kommunicera "fullt ut" med varandra innan den externa uppställningen kan få tillgång till informationen i den portabla databäraren. Slutligen innebär det ovan beskrivna att det biometriska templatet som är lagrat i den portabla databäraren aldrig behöver lämna bärarminnet eftersom att jämförelsen med det biometriska provet sker i den portabla databäraren. Den portabla databäraren är i föreliggande utföringsform närmare bestämt anordnad att förhindra åtkomst till det biometriska templatet varvid det således är skyddat från all läsning av externa uppställningar.

Den portabla databäraren i den ovan beskrivna utföringsformen är en passiv databärare i form av ett elektroniskt pass. I en alternativ utföringsform är den portabla databäraren istället en aktiv databärare i form av en mobiltelefon eller en PDA med bankkortsfunktionalitet. Konstruktionen av den aktiva databäraren överensstämmer med konstruktionen av den passiva databäraren enligt fig 1 förutom att den aktiva databäraren även innefattar en energikälla för kraftsättning av de ingående komponenterna. Den aktiva databäraren och en extern uppställning likt den ovan beskrivna enligt fig 2 ingår i ett system i vilket de är anordnade att kontaktlöst kommunicera med varandra enligt någon känd kommunikationsteknik, t ex Bluetooth. Precis som i utföringsformen ovan svarar det i den aktiva databäraren lagrade biometriska templatet mot data för ett fingeravtryck från den aktiva databärarens rättmätige innehavare. Den i den aktiva databäraren lagrade tillämpningsspecifika funktionen innefattar en uppsättning instruktioner enligt vilka den aktiva databärar-

en är anordnad att arbeta som svar på en från den externa uppställningen mottagen förfrågan. I denna utföringsform omfattar den tillämpningsspecifika funktionen instruktioner som lämpar sig för en bankkortstillämpning, såsom t ex att verifiera från den externa uppställningen mottagna data och signera en penningtransaktion. Detta skall göras under förutsättning att biometrisk matchning har konstaterats, handskakning har utförts med den externa uppställningen och en förfrågan har tagits emot från den externa uppställningen. Precis som i utföringsformen ovan är den externa uppställningen anordnad att med hjälp av en sensor registrera ett biometriskt prov svarande mot data för ett fingeravtryck från den person som bär den aktiva databäraren.

När en användare gör ett bankärende med hjälp av sin aktiva databärare utförs en metod liknande den som beskrivs ovan med hänvisning till fig 3 och 4. Användaren närmar sig den externa uppställningen vid vilken bankärendet skall utföras varvid en söksignal och en närvarosignal överförs mellan den aktiva databäraren och den externa uppställningen. Användaren placerar sitt finger på sensorn för registrering av det biometriska provet, vilket därefter trådlöst sänds till den aktiva databäraren. Den aktiva databäraren jämför det mottagna biometriska provet med det biometriska templatet och konstaterar att det föreligger en matchning mellan dessa. Handskakning utförs varvid det verifieras att den aktiva databäraren och den externa uppställningen är avsedda att kommunicera "fullt ut" med varandra. Den externa uppställningen sänder därefter en förfrågan till den aktiva databäraren om att verifiera vissa data och sedan signera den applikation som bankärendet avser. Denna signering blir det resultat som överförs från den aktiva databäraren till den externa uppställningen innan kommunikationen dem emellan avbryts. Bankärendet är därmed utfört.

Både i samband med utföringsformen av den passiva databäraren och utföringsformen med den aktiva databärar-

en har det beskrivits hur kommunikationslänken till den externa uppställningen bryts automatiskt efter att resultatet av den tillämpningsspecifika funktionen har överförts från databäraren. I fallet med en passiv databärare och en utföringsform utan en sådan automatisk brytning, bryts kommunikationslänken i vilket fall som helst när den passiva databäraren kommer utanför kraftsättningsräckvidden för den externa uppställningen eftersom den passiva databärarens kraftsättning då upphör. Detta sker dock inte i en liknande utföringsform med en aktiv databärare eftersom denna har sin egen kraftkälla. För att öka säkerheten mot obehörig läsning kan den aktiva databäraren vara anordnad att, med jämna mellanrum efter att överföringen av resultatet har påbörjats, kontrollera om en förutbestämd överföringstid har förflutit. När kontrollen ger att den förutbestämda överföringstiden har förflutit är den aktiva databäraren sedan anordnad att avbryta kommunikationen med den externa uppställningen.

Även om speciella utföringsformer av uppfinningen har beskrivits ovan så är det uppenbart för fackmannen att många alternativ, modifieringar och variationer är möjliga att åstadkomma i ljuset av ovanstående beskrivning. Exempel på sådana alternativ diskuteras nedan.

I ovanstående utföringsform med den passiva databäraren har det antagits att den externa uppställningens kommunikationsräckvidd är den samma som räckvidden för kraftsättning av den passiva databäraren. I en annan utföringsform av uppfinningen är räckvidden för kraftsättning av den passiva databäraren inte densamma som kommunikationsräckvidden. I ytterligare en annan utföringsform kraftsätts den passiva databäraren inte med hjälp av den externa uppställningen. Istället sker dess kraftsättning med hjälp av separata enheter i den externa uppställningens omgivning. Sådana separata kraftsättningsenheter skulle t ex kunna vara anordnade på olika strategiska positioner i ett utrymme där även den externa uppställningen är anordnad. I en sådan utföringsform skulle den

passiva databäraren kraftsättas så snart dess bärare träder in i utrymmet.

I enlighet med alternativa utföringsformer till de ovan beskrivna utelämnas stegen för utsändning av söksignal, kontroll av mottagning av söksignal, utsändning av närvarosignal och kontroll av mottagning av närvarosignal (U1, B1, B2, U2 i systemförfarandet enligt fig 3 och 4). Denna utföringsform innebär att den externa uppställningen är anordnad att registrera ett biometriskt prov och sända ut detta enligt ett förutbestämt schema, t ex med bestämda intervaller, tills matchning med en portabel databärare anses föreligga. Denna utföringsform innebär vidare att den portabla databäraren, utan att avslöja sin närvaro inom en kommunikationsräckvidd för den externa uppställningen, är anordnad att ta emot det biometriska provet och göra en jämförelse med det i bärarminnet lagrade biometriska templatet. I detta fall är alltså den portabla databäraren anordnad att förhindra all utsändning av data från densamma tills matchning med ett biometriskt prov anses föreligga. Denna utföringsform medför att det biometriska prov som registreras av den externa uppställningen sänds till samtliga portabla databärare inom den externa uppställningens kommunikationsräckvidd men att bara den portabla databärare vilken har ett lagrat biometriskt templat som matchar det biometriska provet avslöjar sin närvaro för den externa uppställningen. Genom denna utföringsform kan således blotta innehavet av en portabel databärare enligt uppfinningen hemlighållas om innehavaren så önskar.

I ovanstående utföringsformer är konstruktionen sådan att kommunikationen mellan den portabla databäraren och den externa uppställningen avbryts och måste återinitieras om databäraren av någon anledning under en kort stund lämnar kommunikationsräckvidden. I enlighet med en alternativ utföringsform tillhandahålls en kommunikationsåterupptagningsmöjlighet som innebär att kommunikationen kan återupptas från det "ställe" där den avbröts

såvida databäraren inte lämnar kommunikationsräckvidden under en tid som överstiger en förutbestämd maxtid.

I ovanstående utföringsformer utförs handskakningsproceduren mellan den portabla databäraren och den externa uppställningen efter att biometrisk matchning har konstaterats. Enligt alternativa utföringsformer kan denna handskakningsprocedur istället utföras innan den biometriska matchningen.

I ovanstående utföringsformer är den portabla databäraren anordnad att utföra den tillämpningsspecifika funktionen och överföra ett resultat av densamma till den externa uppställningen under villkoren att biometrisk matchning har konstaterats, handskakning har utförts och en förfrågan har tagits emot. Alternativa utföringsformer är möjliga i vilka fler villkor måste vara uppfyllda för utförande av den tillämpningsspecifika funktionen och översändande av resultatet. I en utföringsform utförs exempelvis en kompletterande identitetskontroll efter att biometrisk matchning har konstaterats genom jämförelsen i den portabla databäraren. Denna kompletterande kontroll kan antingen göras i den portabla databäraren eller i den externa uppställningen och t ex innefatta verifieringen av en hemlig kod eller utförandet av ytterligare en biometrisk matchning.

Uppfinningen är avsedd att omfatta alla möjliga alternativ, modifieringar och variationer av ovanstående utföringsformer som faller inom ramen för de bifogade kraven.

PATENTKRAV

1. Portabel databärare (10) vilken omfattar ett bärarminne (12) för lagring av data innefattande ett biometriskt templat (13) och en tillämpningsspecifik funktion (15) samt bärarkommunikationsorgan (11) för att kontaktfritt ta emot och sända ut data, k ä n n e t e c k n a d av att den vidare omfattar bärarbehandlingsorgan (16) för att jämföra det biometriska templatet med ett från en extern uppställning (20) mottaget biometriskt prov (23) och är anordnad att utföra den tillämpningsspecifika funktionen och sända ett resultat av densamma till den externa uppställningen endast om det biometriska provet matchar det biometriska templatet.

2. Portabel databärare (10) enligt krav 1, varvid den tillämpningsspecifika funktionen (15) omfattar att från bärarminnet (12) hämta däri lagrad tillämpningsspecifik information (14), varvid nämnda resultat innefattar den tillämpningsspecifika informationen.

3. Portabel databärare (10) enligt något av ovanstående krav, varvid den tillämpningsspecifika funktionen (15) omfattar att exekvera i bärarminnet (12) lagrad programkod.

4. Portabel databärare (10) enligt något av ovanstående krav, anordnad att utföra den tillämpningsspecifika funktionen (15) samt sända nämnda resultat av densamma till den externa uppställningen (20) som svar på en från den externa uppställningen mottagen förfrågan.

5. Portabel databärare (10) enligt något av ovanstående krav, varvid det biometriska templatet (13) svarar mot en digital bild innefattande individspecifik information.

6. Portabel databärare (10) enligt något av ovanstående krav, varvid det biometriska templatet (13) definierar åtminstone en del av ett fingeravtryck.

7. Portabel databärare (10) enligt något av ovanstående krav, varvid det biometriska templatet (13) svarar mot särdragsreferensdata.

8. Portabel databärare (10) enligt något av ovanstående krav, anordnad att i bärarminnet (12) lagra ett tröskelvärde som definierar i vilken grad det biometriska provet (23) ska överensstämma med det biometriska (13) templatet för att en matchning ska anses föreligga.

9. Portabel databärare (10) enligt något av ovanstående krav, vilken databärare är ett smartcard.

10. Portabel databärare (10) enligt något av krav 1-8, vilken databärare är ett elektroniskt pass.

11. Portabel databärare (10) enligt något av krav 1-8, vilken databärare är en mobiltelefon.

12. Portabel databärare (10) enligt något av krav 1-8, vilken databärare är en PDA ("Personal Digital Assistant").

13. Portabel databärare (10) enligt något av ovanstående krav, anordnad att för den externa uppställningen (20) förhindra åtkomst till det biometriska templatet (13).

14. Portabel databärare (10) enligt något av ovanstående krav, anordnad att kommunicera med den externa uppställningen (20) endast under en förutbestämd tid efter att matchning har ansetts föreligga.

15. Portabel databärare (10) enligt något av ovanstående krav, anordnad att sända ut en närvarosignal som svar på en från den externa uppställningen (20) mottagen söksignal för att bekräfta sin närvaro inom en kommunikationsräckvidd för den externa uppställningen.

16. Portabel databärare (10) enligt något av krav 1-14, anordnad att förhindra all utsändning av data från densamma tills matchning anses föreligga.

17. Förfarande för överföring av data med hjälp av en portabel databärare (10) vilken omfattar ett bärarminne (12) för lagring av data innefattande ett biometriskt templat (13) och en tillämpningsspecifik funktion

(15) samt bärarkommunikationsorgan (11) för att kontaktfritt ta emot och sända ut data, k ä n n e t e c k n a t av

att ta emot ett biometriskt prov (23) från en extern uppställning (20) (B3),

att med hjälp av bärarbehandlingsorgan (16) i databäraren jämföra det biometriska provet med det biometriska templatet (B4), och

att utföra den tillämpningsspecifika funktionen och sända ett resultat av densamma till den externa uppställningen (B10) endast om det biometriska provet matchar det biometriska templatet.

18. Förfarande enligt krav 17, varvid att utföra den tillämpningsspecifika funktionen (15) omfattar att från bärarminnet (12) hämta däri lagrad tillämpningsspecifik information (14), varvid nämnda resultat innefattar den tillämpningsspecifika informationen.

19. Förfarande enligt något av krav 17-18, varvid att utföra den tillämpningsspecifika funktionen (15) omfattar att exekvera i bärarminnet (12) lagrad programkod.

20. Förfarande enligt något av krav 17-19, innefattande att utföra den tillämpningsspecifika funktionen (15) samt sända nämnda resultat av densamma till den externa uppställningen (20) (B10) som svar på en från den externa uppställningen mottagen förfrågan (B9).

21. Förfarande enligt något av krav 17-20, varvid det biometriska templatet (13) svarar mot en digital bild innefattande individspecifik information.

22. Förfarande enligt något av krav 17-21, varvid det biometriska templatet (13) definierar åtminstone en del av ett fingeravtryck.

23. Förfarande enligt något av krav 17-22, varvid det biometriska templatet (13) svarar mot särdragsreferensdata.

24. Förfarande enligt något av krav 17-23, vidare innefattande att bedöma ett resultat av jämförelsen mot ett i bärarminnet lagrat tröskelvärde som definierar i

vilken grad det biometriska provet ska överensstämma med det biometriska templatet för att en matchning ska anses föreligga (B5).

25. Förfarande enligt något av krav 17-24, varvid databäraren (10) är ett smartcard.

26. Förfarande enligt något av krav 17-24, varvid databäraren (10) är ett elektroniskt pass.

27. Förfarande enligt något av krav 17-24, varvid databäraren (10) är en mobiltelefon.

28. Förfarande enligt något av krav 17-24, varvid databäraren (10) är en PDA ("Personal Digital Assistant").

29. Förfarande enligt något av krav 17-28, vidare innefattande att hindra kommunikation med den externa uppställningen (20) när en förutbestämd tid, efter att matchning har ansetts föreligga (B5), har förflutit.

30. Förfarande enligt något av krav 17-29, vidare innefattande att ta emot en söksignal från den externa uppställningen (20) (B1) och att som svar på söksignalen sända ut en närvarosignal (B2) för att bekräfta sin närvaro inom en kommunikationsräckvidd för den externa uppställningen.

31. Förfarande enligt något av krav 17-29, vidare innefattande att förhindra all utsändning av data från den portabla databäraren (10) tills matchning anses föreligga (B5).

32. Minnesmedium innefattande ett datorprogram med instruktioner vilka är anordnade att vid exekvering utföra förfarandet enligt något av kraven 17-31.

33. Extern uppställning (20) innefattande uppställningskommunikationsorgan (21) för att kontaktfritt ta emot och sända ut data samt en sensor (25) för att registrera ett biometriskt prov (23), k ä n n e t e c k n a d av att av att den är anordnad att sända det biometriska provet till en portabel databärare (10) och ta emot, endast om det biometriska provet matchar ett i den portabla databäraren lagrat biometriskt templat (13), ett

resultat av en i den portabla databäraren utförd tillämpningsspecifik funktion (15) från databäraren.

34. Extern uppställning (20) enligt krav 33, anordnad att som nämnda resultat ta emot i databäraren lagrad tillämpningsspecifik information (14).

35. Extern uppställning (20) enligt något av krav 33-34, anordnad sända en förfrågan till den portabla databäraren (10) och att ta emot nämnda resultat som svar på denna förfrågan.

36. Extern uppställning (20) enligt något av krav 33-35, varvid det biometriska provet (23) svarar mot en digital bild innefattande individspecifik information.

37. Extern uppställning (20) enligt något av krav 33-36, varvid det biometriska provet (23) definierar åtminstone en del av ett fingeravtryck.

38. Extern uppställning (20) enligt något av krav 33-37, varvid det biometriska provet (23) svarar mot särdragsdata.

39. Extern uppställning (20) enligt något av krav 33-38, anordnad att sända ut en söksignal och som svar på söksignalen ta emot en närvarosignal från den portabla databäraren (10) för att detektera dess närvaro inom en kommunikationsräckvidd för den externa uppställningen.

40. Extern uppställning (20) enligt något av krav 33-39, anordnad att sända ut det biometriska provet (23) enligt ett förutbestämt schema tills matchning anses föreligga.

41. Förfarande för överföring av data med hjälp av en extern uppställning (20) vilken innefattar uppställningskommunikationsorgan (21) för att kontaktfritt ta emot och sända ut data samt en sensor (25), innefattande att med hjälp av sensorn registrera ett biometriskt prov (23) (U3), k ä n n e t e c k n a t av att det vidare innefattar

att sända det biometriska provet till en portabel databärare (10) (U4), och

att ta emot, endast om det biometriska provet matchar ett i den portabla databäraren lagrat biometriskt template (13), ett resultat av en i den portabla databäraren utförd tillämpningsspecifik funktion (15) från databäraren (U10).

42. Förfarande enligt krav 41, innefattande att som nämnda resultat ta emot i databäraren (10) lagrad tillämpningsspecifik information (14) (U10).

43. Förfarande enligt något av krav 41-42, vidare innefattande att sända en förfrågan till den portabla databäraren (10) (U9) och att ta emot nämnda resultat som svar på denna förfrågan (U10).

44. Förfarande enligt något av krav 41-43, vidare innefattande att sända ut en söksignal (U1) och att som svar på söksignalen ta emot en närvarosignal (U2) från den portabla databäraren (10) för att detektera dess närvaro inom en kommunikationsräckvidd för den externa uppställningen (20).

45. Förfarande enligt något av krav 41-44, vidare innefattande att sända ut det biometriska provet enligt ett förutbestämt schema tills matchning anses föreligga.

46. Minnesmedium innefattande ett datorprogram med instruktioner vilka är anordnade att vid exekvering utföra förfarandet enligt något av kraven 41-45.

47. System för överföring av data innefattande en portabel databärare (10) enligt något av krav 1-16 och en extern uppställning (20) enligt något av krav 33-40.

48. Förfarande för överföring av data innefattande ett förfarande enligt något av krav 17-31 och ett förfarande enligt något av krav 41-45.

SAMMANDRAG

En portabel databärare (10) och ett förfarande (B1-B10), samt ett minnesmedium med instruktioner, för överföring av data med hjälp av en portabel databärare tillhandahålles. Den portabla databäraren omfattar ett bärarminne (12) för lagring av data innefattande ett biometriskt templat (13) och en tillämpningsspecifik funktion (15) samt bärarkommunikationsorgan (11) för att kontaktfritt ta emot och sända ut data. Den portabla databäraren kännetecknas av att den vidare omfattar bärarbehandlingsorgan (16) för att jämföra det biometriska templatet med ett från en extern uppställning (20) mottaget biometriskt prov (23) och av att den är anordnad att utföra den tillämpningsspecifika funktionen och sända ett resultat av densamma till den externa uppställningen endast om det biometriska provet matchar det biometriska templatet.

Publiceringsbild: Fig 3

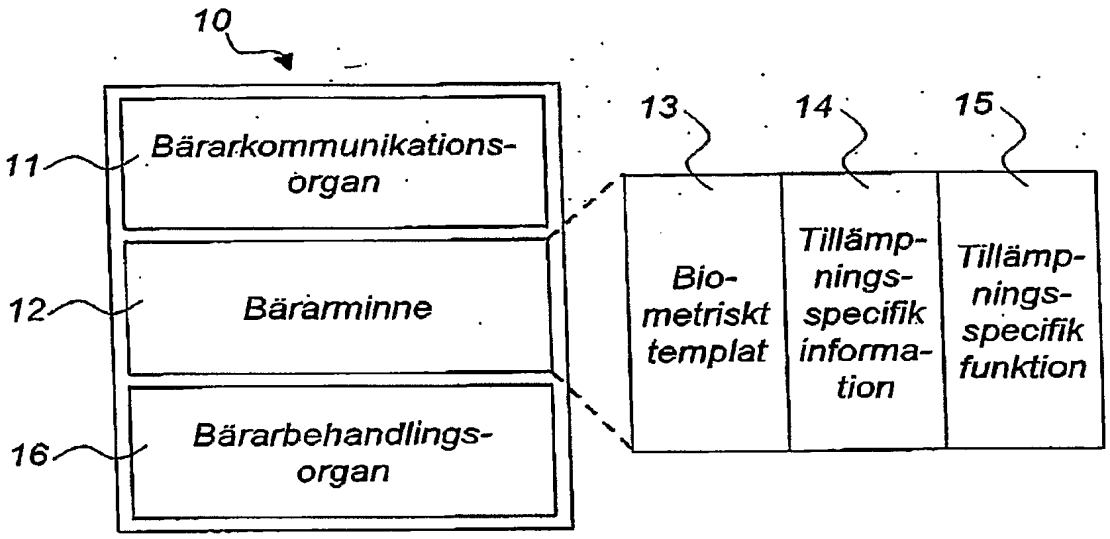
10
11
Bärarkommunikations-organ
12
Bärarminne
16
Bärarbehandlings-organ
13
14
15
Bio-metriskt templat
Tillämp-nings-specifik informa-tion
Tillämp-nings-specifik funktion

Fig 1

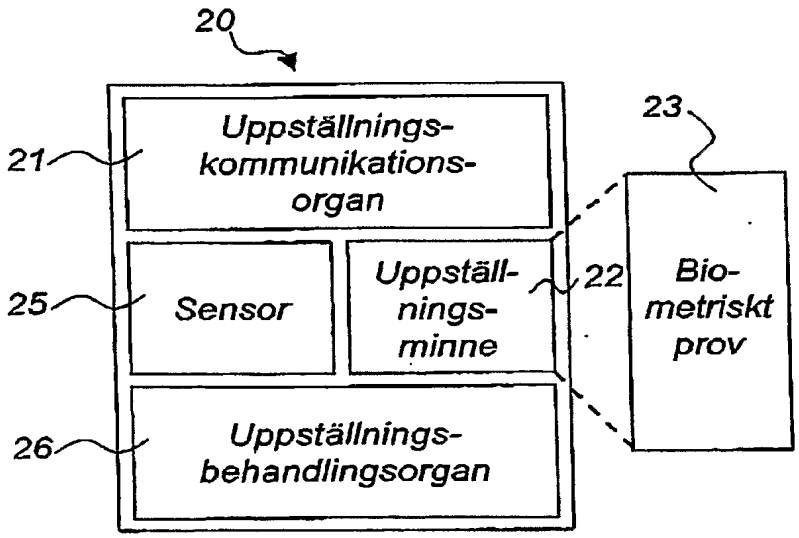
20
21
Uppställnings-kommunikations-organ
25
Sensor
Uppställ-nings-minne
22
26
Uppställnings-behandlingsorgan
23
Bio-metriskt prov

Fig 2

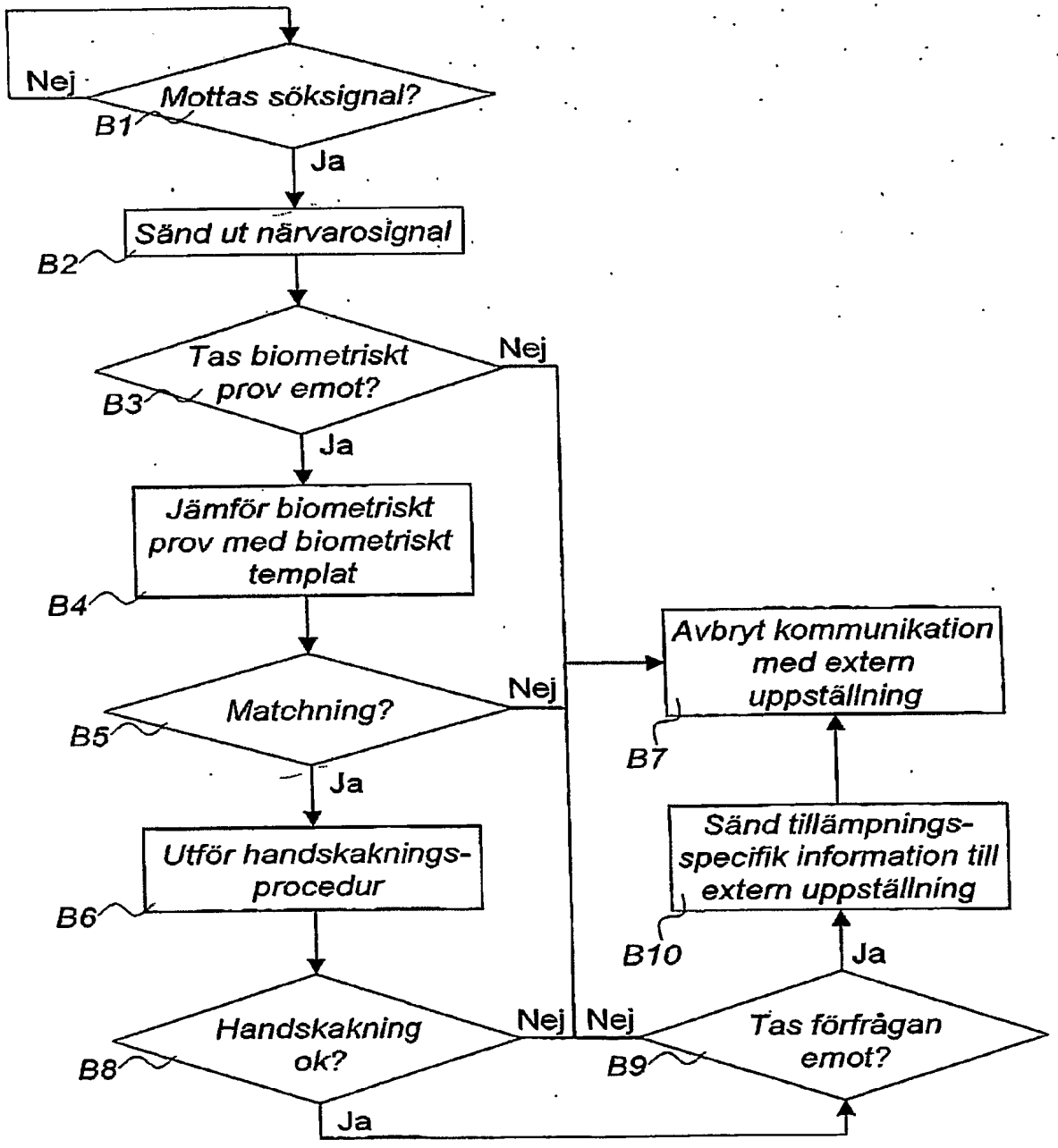
Nej
Mottas söksignal?
B1
Ja
Sänd ut närvarosignal
B2
Tas biometriskt prov emot?
B3
Nej
Ja
Jämför biometriskt prov med biometriskt templat
B4
Matchning?
B5
Nej
Ja
Utför handskakningsprocedur
B6
Handskakning ok?
B8
Nej
Ja
Avbryt kommunikation med extern uppställning
B7
Sänd tillämpningsspecifik information till extern uppställning
B10
Tas förfrågan emot?
B9
Nej
Ja

Fig 3

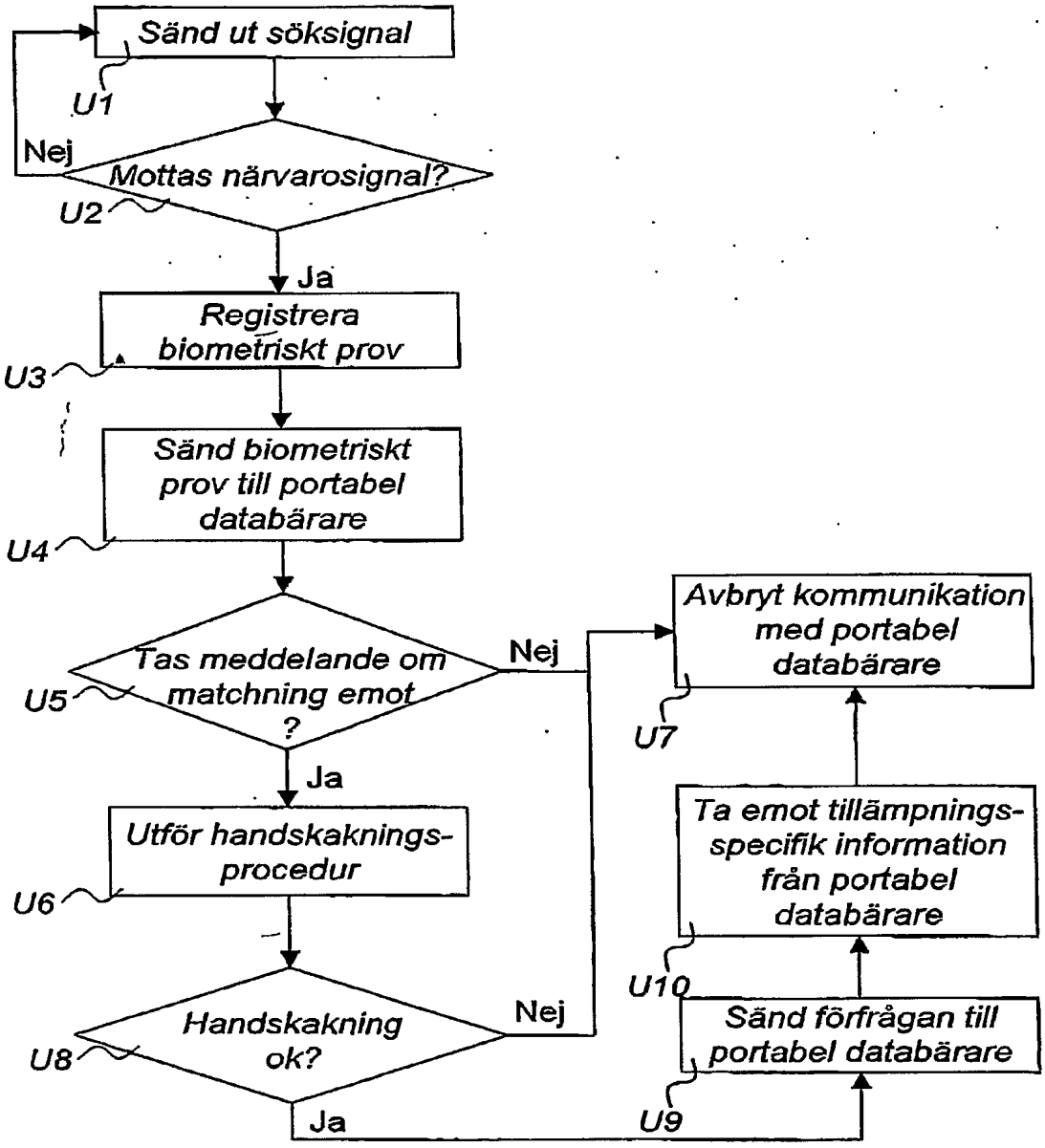
Sänd ut söksignal
U1
Nej
Mottas närvarosignal?
U2
Ja
Registrera biometriskt prov
U3
Sänd biometriskt prov till portabel databärare
U4
Tas meddelande om matchning emot ?
U5
Nej
Ja
Utför handskakningsprocedur
U6
Handskakning ok?
U8
Nej
Ja
Avbryt kommunikation med portabel databärare
U7
Ta emot tillämpningsspecifik information från portabel databärare
U10
Sänd förfrågan till portabel databärare
U9

Fig 4